Abstract

A method for establishing a common key for a group of at least three subscribers includes using a publicly known mathematical number group and a higher order element of the group $g \in G$. In the first step, a message corresponding to $Ni: = g^{zi}$ mod p is sent by each subscriber to all other subscribers (Tj), (zi) being a random number chosen from the set (1, ..., p-2) by a random number generator. In the second step, each subscriber (Ti) selects a transmission key $kij: = (g^{zj})^{zi}$ for each other subscriber (Tj) from the received message (g^{zj}), with $i \neq j$, for transmitting their random number (zi) to the subscribers (Tj). In the third step, the common key k is calculated as k: = f(z1, z2, ..., zn) for each subscriber Ti.